Patch Release Note

Patch 86253-03
For Rapier Series Switches

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86253-03 for Software Release 2.5.3 on existing models of Rapier series switches. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86253-03.

Base Software Release File	86s-253.rez
Patch Release Date	30-July-2003
Compressed Patch File Name	86253-03.paz
Compressed Patch File Size	191102 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.5.3 for Rapier Switches and AR400 and AR700 Series Routers (Document Number C613-10362-00 Rev A) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Rapier Switch Documentation Set for Software Release 2.5.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Features in 86253-03

Patch 86253-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.3, and the following enhancements:

PCR: 03816 Module: IPG Level: 2

When ports were added or removed as a range with the ENABLE IP IGMP ALLGROUPS and DISABLE IP IGMP ALLGROUPS commands, port values were interpreted as 2 separate ports. This issue has been resolved.

Features in 86253-02

Patch file details are listed in Table 2:

Table 2: Patch file details for Patch 86253-02.

Base Software Release File	86s-253.rez
Patch Release Date	25-July-2003
Compressed Patch File Name	86253-02.paz
Compressed Patch File Size	190900 bytes

Patch 86253-02 includes the following enhancements and resolved issues:

PCR: 03420 Module: IPG, SWI Level: 3

It is now possible to prevent specified ports from acting as IGMP all-group ports, and specify which ports are allowed to behave as all-group entry ports. This is enabled with the ENABLE IP IGMP ALLGROUP command, and disabled with the DISABLE IP IGMP ALLGROUP command.

For details, see "*IGMP Snooping All-Group Entry*" on page 5.

PCR: 03515 Module: DHCP Level: 3

DHCP was offering network and broadcast addresses to clients. This issue has been resolved.

PCR: 03609 Module: OSPF Level: 1

The IP route filter did not always work correctly for OSPF. This issue has been resolved.

PCR: 03657 Module: SWI Level: 3

Executing the DISABLE SWITCH PORT command on a port that was the source of a mirror port did not disable the mirror port. This issue has been resolved.

PCR: 03691 Module: DVMRP Level: 2

A fatal error occurred if the number of DVMRP interfaces being added exceeded the limit. This issue has been resolved.

PCR: 03692 Module: BGP Level: 2

Occasionally a fatal exception may have occurred when sending BGP aggregate routes. This issue has been resolved.

PCR: 03696 Module: IPG Level: 2

IGMP snooping entries were not being deleted from the hardware table. This issue has been resolved. Also, port timers are now updated when the IGMP timeout is changed.

PCR: 03698 Module: DVMRP Level: 3

The output of the SHOW DVMRP FORWARDING command did not display the forwarding ports. This issue has been resolved.

PCR: 03707 Module: STP Level: 2

When adding a port to a VLAN, any STP ports that had been disabled in the default STP were re-enabled. This issue has been resolved.

PCR: 03708 Module: DHCP Level: 2

When the DELETE DHCP RANGE command was executed, DHCP attempted to reclaim the addresses in that range. It also tried to reclaim addresses in that range that were not allocated at that time, resulting in duplicate addresses appearing on the free list for allocation. This has been resolved by allowing DHCP to reclaim only those addresses that are currently in use by one of its clients.

PCR: 03720 Module: STP Level: 2

When changing from RSTP to STP mode, the STPCOMPATIBLE option for the RSTPTYPE parameter incorrectly appeared in the dynamic configuration. Also, when changing from RSTP to STP mode or vice versa, disabled STP ports did not remain in the disabled state. These issues have been resolved.

PCR: 03738 Module: IPG Level: 2

If a port went down, the port was deleted from the appropriate static IGMP associations but was not added back again when it came back up. Similarly, static IGMP associations were automatically deleted but not added back when IP or IGMP was disabled. These issues have been resolved. You can now create IGMP associations before enabling IGMP, and they will become active when IGMP is enabled.

PCR: 03741 Module: FIREWALL Level: 3

The maximum number of firewall sessions had decreased since software release 86s-241. This issue has been resolved.

PCR: 03742 Module: IPV6 Level: 2

Previously, an incorrect source address was used for router advertisements that were sent over an IPv6 tunnel. The source address of the tunnel (specified by the IPADDRESS parameter of the ADD IPV6 TUNNEL command) was used instead of a link local address. This caused an interoperability problem, which has been resolved. Now, if the specified IP address is not a link local address, then a link local address will be created based on the IPv4 tunnel source address and used for router advertisements.

PCR: 03743 Module: IP Level: 3

If a ping was active and the IP configuration was reset, subsequent pings were sent out the wrong interface. This issue has been resolved.

PCR: 03744 Module: PING Level: 3

Executing a ping to the IP address 0.0.0.0 did not return an `invalid destination address` error message. Also, when the TRACE command was executed for local addresses, it timed out after 90 seconds. These issues have been resolved.

PCR: 03764 Module: IPG Level: 3

The IP multicast counter did not increment when IGMP, DVMRP and PIM packets were transmitted and received. This issue has been resolved.

PCR: 03766 Module: FIREWALL Level: 2

The firewall denied streaming data using Windows Media Player 9. This issue has been resolved.

PCR: 03779 Module: DHCP Level: 2

The DHCP client was not honouring a subnet option provided by the DHCP server. This issue has been resolved.

PCR: 03783 Module: IPG Level: 3

The TIMEOUT and SIZE parameters are only valid for the SET IP DNS CACHE command, but no error message was returned if either parameter was specified for the SET IP DNS command. This issue has been resolved.

PCR: 03784 Module: IPV6 Level: 3

Fragmentation of IPv6 packets now complies with RFC 2460's requirement to align packet sizes to 8 octets.

PCR: 03788 Module: DHCP Level: 2

The DHCP server did not send a *DHCPNAK* message when a previously statically assigned IP DHCP entry was again requested by a client. This issue has been resolved.

PCR: 03793 Module: RSVP Level: 3

The ENABLE RSVP INTERFACE command did not succeed if IP was enabled after the RSVP interface had been created. Now, ENABLE RSVP INTERFACE will succeed regardless of when IP is enabled as long as an IP interface exists.

PCR: 03799 Module: DHCP Level: 3

When a new static entry was allocated to a client, an old dynamic entry remained *inuse* for a full lease period. This issue has been resolved. The old entry will now be reclaimed when the client attempts to renew its lease and receives the new static entry.

IGMP Snooping All-Group Entry

Because IGMP is an IP-based protocol, multicast group membership for VLAN aware devices is on a per-VLAN basis. If at least one port in the VLAN is a member of a multicast group, multicast packets will be flooded onto all ports in the VLAN by default.

IGMP snooping enables the switch to forward multicast traffic intelligently on the switch. The switch listens to IGMP membership reports, queries and leaves messages to identify the switch ports that are members of multicast groups. Multicast traffic will only be forwarded to ports identified as members of the specific multicast group.

This enhancement allows network managers to prevent specified ports from acting as IGMP all-group ports, and specify which ports are allowed to behave as all-group entry ports, by using the ENABLE IP IGMP ALLGROUP command.

For example, consider a video streaming service which has 15 channels. When the switch receives IGMP membership reports destined for the address 239.0.0.2 from an unauthorised user, all 15 channels of multicast data floods to that port, which may affect the service of the network. In order to avoid this, the network manager decides whether or not to allow a particular port to behave as an IGMP all-group port, e.g. port 8. Then, whenever the above IGMP membership report is sent, the switch will not automatically add port 8 as one of the egress ports for any IGMP membership report group, so video streaming will not get forwarded to disabled all-group ports selected by the network manager.

Commands

This enhancement modifies one command:

- SHOW IP IGMP

and has two new commands:

- ENABLE IP IGMP ALLGROUP
- DISABLE IP IGMP ALLGROUP

Modified Command

SHOW IP IGMP

Syntax SHOW IP IGMP [COUNTER] [INTERFACE=*interface*]

Description This command displays information about IGMP, and multicast group membership for each IP interface.

This enhancement includes the line “**Disabled All-groups ports**” on the output of this command, as show in Figure 1 on page 6. Ports that are disabled have a “#” symbol next to the port number.

Figure 1: Example output from the SHOW IP IGMP command.

```
IGMP Protocol
--------------------------------------------------------------------------------
Status ........................... Enabled
Default Query Interval ........... 125 secs
Default Timeout Interval ......... 270 secs
Disabled All-groups ports ........ 1,5,7

Interface Name .......... vlan2 (DR)
IGMP Proxy .............. Off
Group List .............

  Group. 238.0.1.2          Last Adv. 172.50.2.1         Refresh time 34 secs
  Ports 3,11,23

  Group. 224.1.1.2          Last Adv. 172.50.2.1         Refresh time 130 secs
  Ports 2,11,23

  All Groups                Last Adv. 172.50.1.1         Refresh time 45 secs
  Ports 1#,11,23


Interface Name .......... vlan4            (DR)
IGMP Proxy .............. Off
Group List .............
  No group memberships.

--------------------------------------------------------------------------------
```

Table 3: New parameter in the output of the SHOW IP IGMP command.

Parameter	Meaning
Disabled All-groups ports	A list of ports that are prevented from behaving as IGMP all-group ports.

Examples To show information about IGMP, use the command:

```
SHOW IP IGMP
```

See Also ENABLE IP IGMP ALLGROUP
DISABLE IP IGMP ALLGROUP

New Commands

This enhancement request introduces two new commands from enabling/ disabling all-group entries on switch ports.

ENABLE IP IGMP ALLGROUP

Syntax `ENABLE IP IGMP ALLGROUP=[{`*`port-list`*`|ALL}]`

where:

- *port-list* is a port number, a range of port numbers (specified as n-m), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 ad end at m, where m is the highest numbered Ethernet switch port, including uplink ports.

Description This command enables the specified port(s) to behave as a multicast all-group ports.

The ALLGROUP parameter specifies the list of ports able to behave as all-group entry ports. If ALL is specified, all ports are able to behave as all-group entry ports. The default is ALL.

Examples To enable ports 1, 5 and 7 to behave as all-group entry ports, use the command:

```
ENABLE IP IGMP ALLGROUP=1,5,7
```

See Also DISABLE IP IGMP ALLGROUP
SHOW IP IGMP

DISABLE IP IGMP ALLGROUP

Syntax `DISABLE IP IGMP ALLGROUP=[{`*`port-list`*`|ALL}]`

where:

- *port-list* is a port number, a range of port numbers (specified as n-m), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet switch port, including uplink ports.

Description This command disables the specified port(s) from acting as a multicast all-group entry ports. Ports that are disabled have a “#” symbol next to the port number in the output of the SHOW IP IGMP command.

Examples To prevent ports 1, 5 and 7 from behaving as all-group entry ports, use the command:

```
DISABLE IP IGMP ALLGROUP=1,5,7
```

See Also ENABLE IP IGMP ALLGROUP
SHOW IP IGMP

Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at *www.alliedtelesyn.co.nz/support/updates/patches.html*. A licence or password is not required to use a patch.